TP n°1 – Introduction Réseaux

1. ipconfig

- A l'aide de la commande `ipconfig /all` que vous lancerez dans une invite de commandes, découvrez l'adresse mac (ou adresse physique) de votre carte réseau.
- Comment est construite cette adresse mac ? Quelles sont les similitudes que vous trouvez entre votre adresse mac et celle des ordinateurs de votre salle de TP ?
- Quel est le constructeur de votre carte réseau ? Vous pouvez le déduire à partir de l'adresse mac. Allez sur le site http://standards.ieee.org/develop/regauth/oui/oui.txt pour trouver la bonne correspondance.
- Quelle est votre adresse IP ? Comparez vos résultats avec ceux des autres étudiants de la salle ? et éventuellement avec les étudiants qui sont connectés via leur portable.
- Si vous déplacez une des machines de la salle pour la connecter chez vous, est-ce que l'adresse mac va changer ? et qu'en est-il de l'adresse IP ?

2. Wireshark

Wireshark est un logiciel de captures et analyseur de trames réseaux. Pour plus d'informations, voir tout d'abord le tutoriel sur Wireshark disponible dans `SupportCours\S2T\M212 Reseau\TP\TP1`

Ouvrez le fichier de capture `osi.pcap` avec le logiciel wireshark.

1 - Combien de trames ont été capturées ?

2 - Pour chacune des trames, vous indiquerez sa taille, le nombre de couches présentes ainsi que pour chaque couche, le protocole réseau associé.

3 – Pour chacune des trames, donnez l'adresse mac source et l'adresse mac destination, ainsi que le type qui apparaît dans l'entête de niveau 2. A quoi correspond ce dernier champ ? Que remarquez-vous au sujet des adresses mac ?

4 – Pour chacune des trames, donnez l'adresse IP source et l'adresse IP destination, ainsi que le protocole qui apparaît dans l'entête IPv4.

5 - Pour chaque protocole listé ci-dessous, indiquez à quelle couche du modèle hybride à 5 couches (physique, liaison, réseau, transport, application) il appartient :

- TCP, ARP, ICMP, UDP, HTTP, FTP, IP, ETHERNET, SSH.

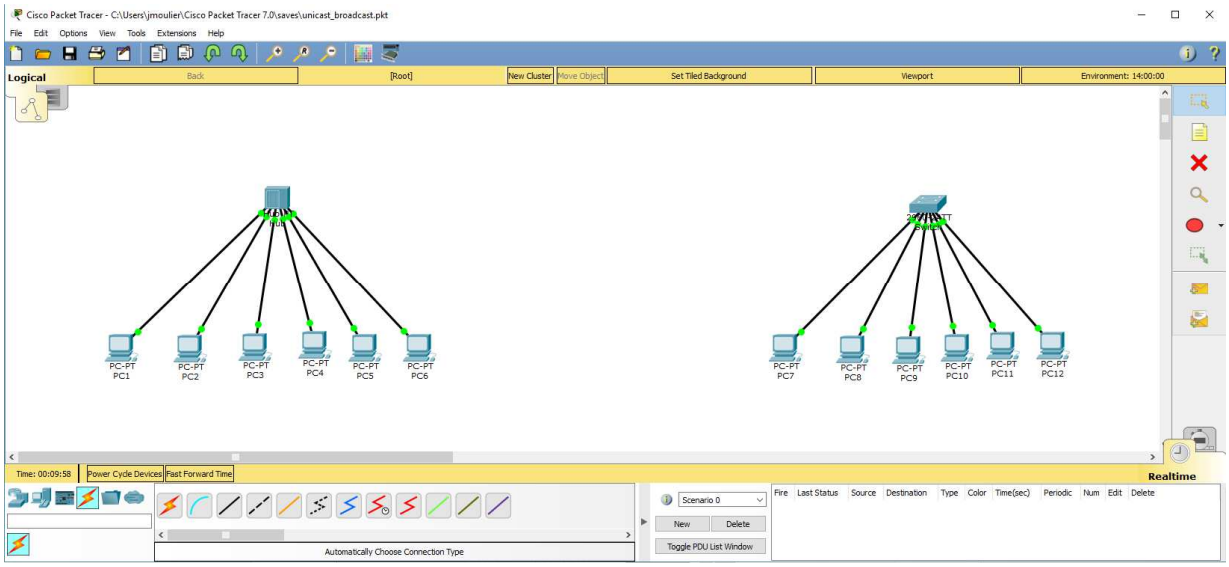
6 - Générez une capture *wireshark* en cliquant sur Capture>Interface (Ctrl+I) puis en choisissant la bonne carte réseau en cliquant sur *start*. De nombreuses trames doivent apparaitre, qui représentent les communications de votre carte réseau. Regardez si les protocoles mentionnés ci-dessus apparaissent dans les trames présentes dans la capture.

7 - Identifiez des paquets http et icmp (vous pouvez utiliser les filtres *wireshark* pour cela, regardez la démonstration de l'enseignant). Si vous ne trouvez pas de tels paquets, essayez de les générer par vous-même en lançant des applications réseaux.

3. PacketTracer : hub et switch

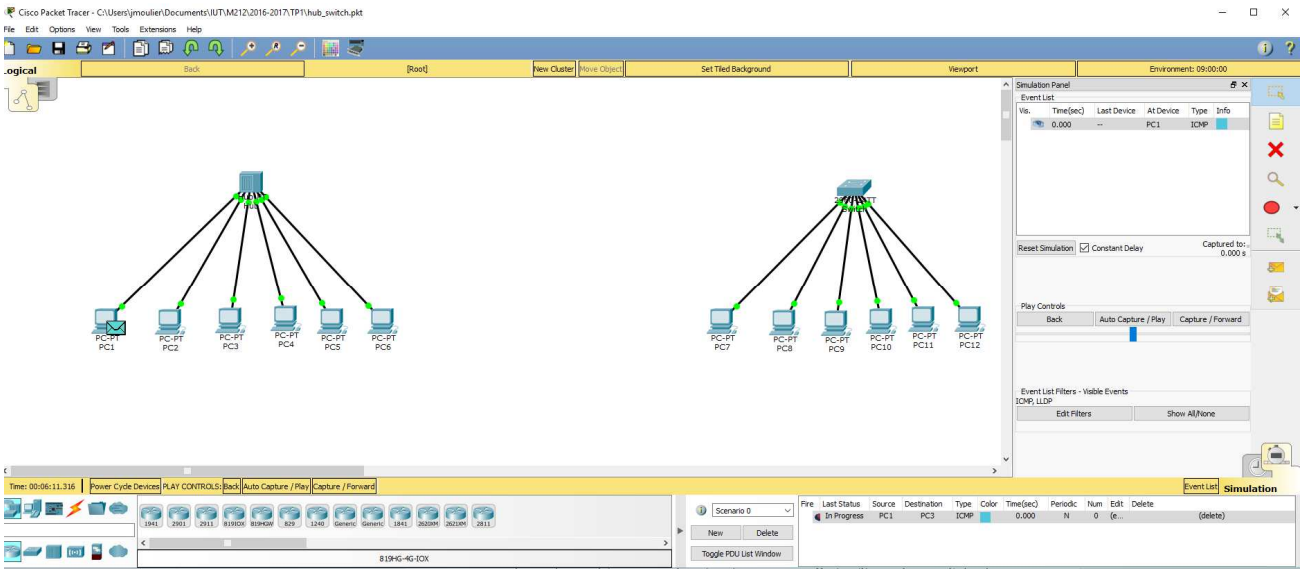
Ouvrez dans packetTracer (situé dans le menu Applications>Réseau) le fichier `hub_switch_6.2.pkt`.

Ce fichier, situé dans `SupportCours\S2T\M212 Reseau\TP\TP1`, est constitué de deux réseaux locaux non connectés entre eux. Le premier est constitué par un hub connecté à 6 machines de PC1 à PC6 pendant que le deuxième est un switch avec les machines PC7 à PC12.



Cliquez sur l'onglet Simulation en bas à droite.

Le panneau de simulation va s'ouvrir :



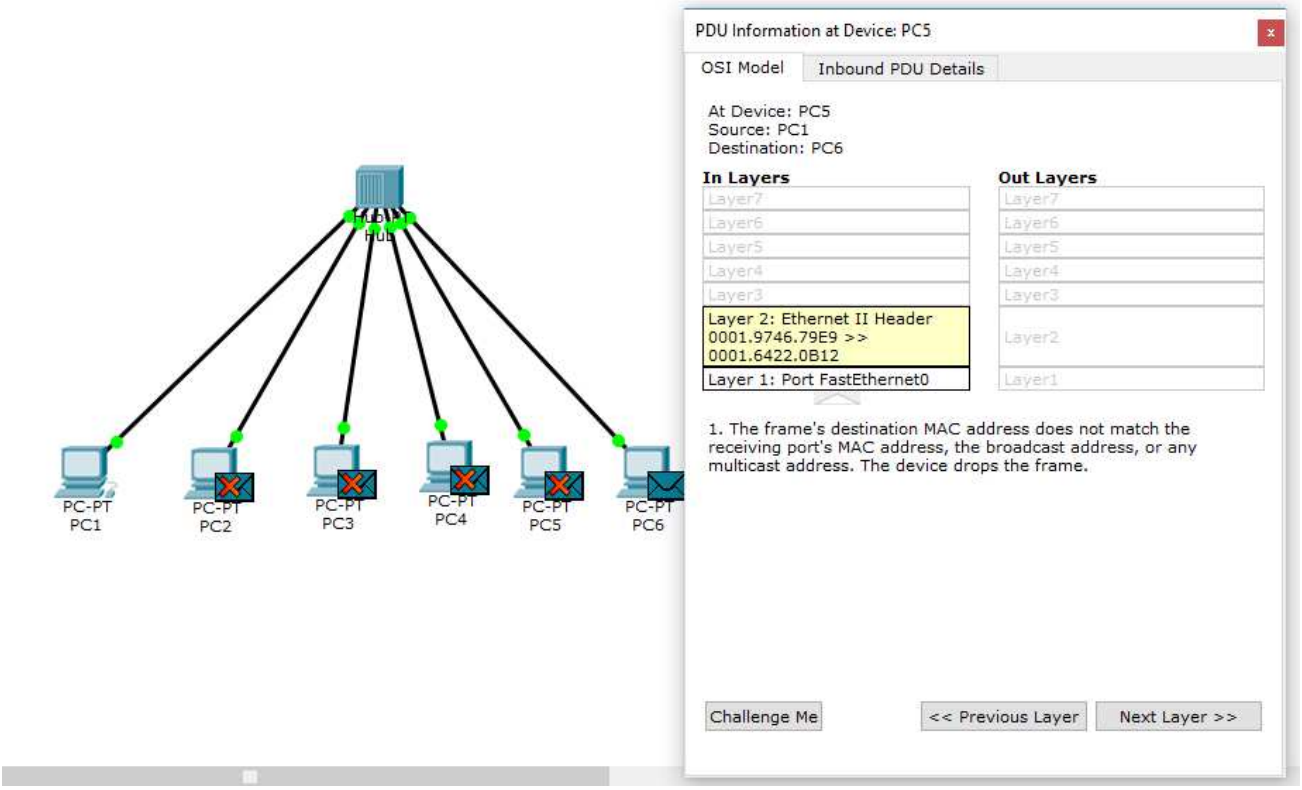
Cliquez sur Show All/none puis sur Edit Filters et sélectionnez uniquement ICMP pour obtenir le même affichage que ci-dessous. On ne capture pour le moment que les messages avec le protocole ICMP (correspondant aux ping).

Vous allez envoyer un message de PC1 vers PC6 (connectés via le hub) puis plus tard de PC7 vers PC9 (connectés via le switch). Il existe plusieurs méthodes pour envoyer un message, vous pouvez notamment cliquer sur l'enveloppe fermée :

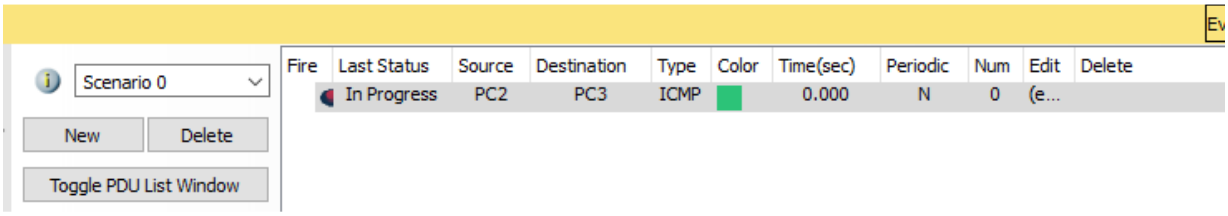
Puis il faut cliquer sur la machine source (exemple PC1) puis la machine destination (exemple PC6).
Une fois que l'enveloppe est mise en attente sur PC1, vous cliquez soit sur Auto Capture/play pour lancer la simulation en mode automatique (puis faire varier le temps éventuellement avec le curseur de simulation pour aller plus ou moins vite), ou sur Capture/Forward pour déclencher manuellement les différentes étapes de la simulation.

Quelles sont vos observations pour ce premier envoi ? Notamment expliquez quelles sont les machines qui ont reçu le message ? quelles sont les machines qui ont lu le message en entier ?

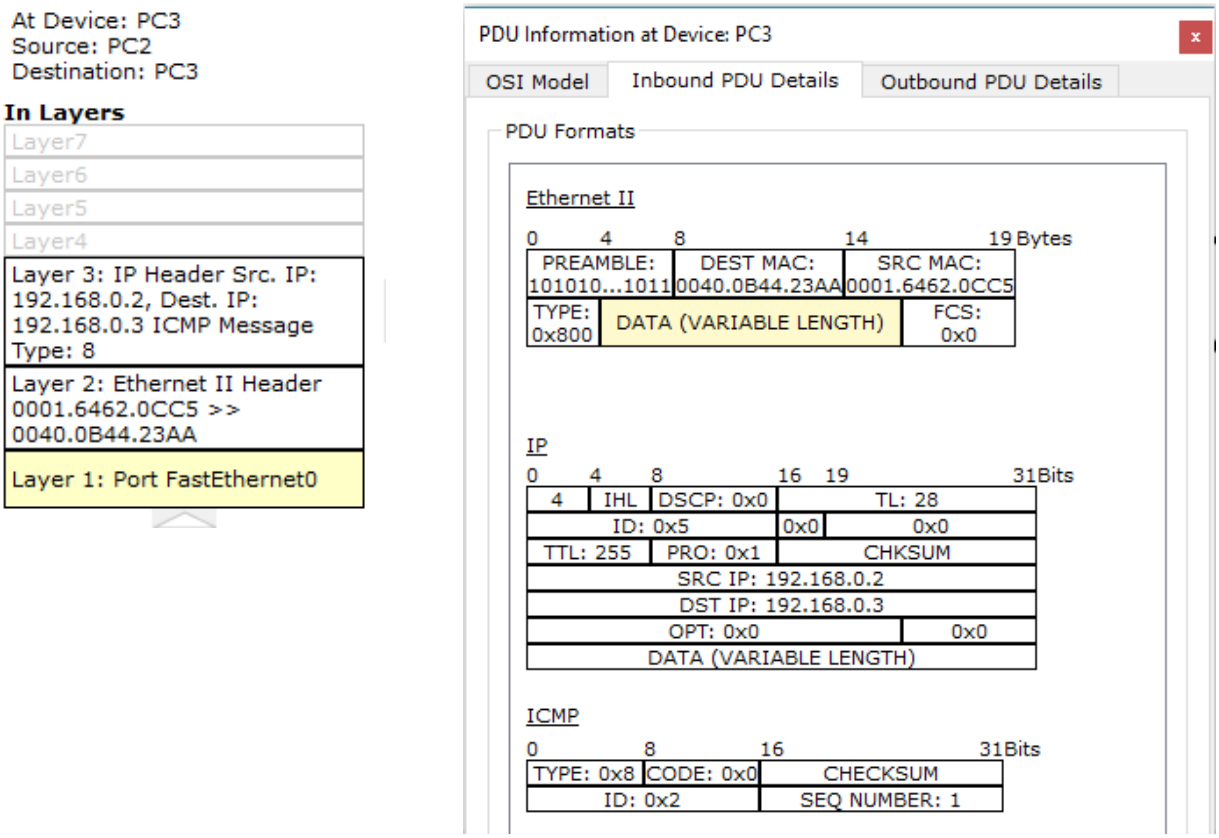
Pour expliquer ce qu'il s'est passé dans le cas de l'envoi du message unicast de PC1 vers PC6, vous allez cliquer sur une des enveloppes détruites (avec la croix rouge). Puis sur *Next Layer* ; cela va vous donner une explication de la destruction du message.



Refaites l'expérience avec le switch, à partir de PC7 et vers PC8 par exemple. Pour annuler une simulation précédente, cliquez sur *delete*, pour ne plus voir d'évènements de simulation dans la liste ci-dessous :



Décrivez la trame Ethernet et ces différents champs correspondant à un échange unicast entre deux machines. Pour cela il faut cliquer sur une enveloppe en cours d'envoi, puis sur *Inbound PDU details* :



Sur quoi se basent les machines pour lire ou non la trame qu'elles reçoivent ? Ou autrement dit pourquoi certaines enveloppes sont-elles détruites dans le cas du hub ?

Tirez les conclusions adéquates en donnant les principales différences entre un hub et un switch. Notamment, répondez aux questions suivantes : Un hub est-il un équipement de la couche liaison ? Permet-il de filtrer les paquets dynamiquement ? Un switch est-il un équipement de la couche liaison ?

Regardez la table mac/port du switch (avec l'outil loupe appliquée sur le switch), combien y-a-t-il d'entrées (de type mac → port) dans cette table ?

MAC Table for Switch

VLAN	Mac Address	Port
1	0001.63BD.D4C8	FastEthernet0/6
1	0004.9A62.D94A	FastEthernet0/1
1	0040.0B13.B1A7	FastEthernet0/4
1	0060.70AA.62D4	FastEthernet0/3
1	0090.0C56.26CA	FastEthernet0/5
1	00E0.F92A.58AE	FastEthernet0/2

Déduisez le nombre d'entrées qu'il faudrait sur ce switch s'il y avait 10000 ordinateurs sur ce réseau local (éventuellement connectées à d'autres switch eux-mêmes reliés entre eux). Ouvrez le fichier `Quatre_switch.pkt` avec packetTracer et confirmez ce que vous venez de déduire.